FUTURE RANGE

PART OF MENTORA GROUP

BOARD ADVISORY PACK

Cyber Security, DORA, NIS2 & GDPR

An independent advisory framework for boards

Boards now carry significant responsibility under DORA, NIS2 and GDPR. This pack outlines a three-step framework for addressing that responsibility, and the independent services from FutureRange that can help deliver on that framework.

Protect · Empower · Evolve

THE BOARD'S POSITION

Cyber risk is now a board-level legal responsibility

DORA and NIS2 places ultimate responsibility for ICT and operational resilience risk squarely on the management body, not the IT team or the institutions managing your assets. GDPR holds the board accountable for the governance of data protection, not just its execution. Directors are answerable, personally and collectively, for risks many were never trained to assess.

The difficulty is structural rather than a failure of diligence. Boards are usually reliant on the very institutions and providers they are meant to oversee, such as asset managers, custodians, IT partners, to confirm that systems are secure and compliant. Policies, certificates and vendor assurances arrive as evidence, but none of them demonstrate that controls work as described. Regulators will not accept "we were told it was fine" as a defence.

Self-reported assurance is not evidence of resilience.

THE RECOMMENDED APPROACH

A board-ready framework: Verify. Remediate. Govern.

1 STEP 01

Verify

Independently confirm the real state of your security posture — and that of every institution and custodian holding your assets or data.

2 STEP 02

Remediate

Close the gaps verification uncovers, guided by a prioritised roadmap mapped against DORA, GDPR, NIS2, ISO 27001, NIST and CIS.

3 STEP 03

Govern

Embed oversight: board reporting, a defined risk appetite and director-level literacy, so assurance becomes routine.

We do not replace your IT partner or team. We independently verify what they tell you and help you act on it.

THE SERVICES BEHIND THE FRAMEWORK

Independent support at every stage

FUTURE RANGE

VERIFY — REMEDIATE — GOVERN

01

VERIFY

Independent Cyber Security Audits

A technical assessment of the controls that actually protect the organisation: identity, endpoints, network, cloud tenancy, backup and recovery; carried out by a third party with no stake in the result.

You receive: a risk-ranked findings report, a two-page executive summary written for the board, and the underlying evidence pack.

Maps to · DORA ICT risk management · ISO 27001 Annex A · NIS2 Art. 21

02

VERIFY

Systems and Evidence Testing

As a Managed Security Services Provider we hold the capability in-house to test systems rather than read about them: penetration testing, vulnerability scanning, configuration audit and compliance testing. We apply it to your own estate and to the institutions, custodians and providers holding your assets or data.

You receive: an evidence-verification matrix per third party, a gap log of unsupported claims, and a custodian assurance summary for the board.

Maps to · DORA third-party risk (Ch. V) · GDPR Art. 28 & 32

03

REMEDIATE

Prioritised & Budgeted Action List

Findings become decisions. Every gap is translated into a named action with an owner, an effort estimate and an indicative budget, sequenced so the highest reduction in risk comes first.

You receive: an action register with owners and effort, an impact-versus-effort ranking, and a short list of quick wins to close immediately.

Maps to · DORA ICT risk framework · NIST CSF · CIS Controls

04

REMEDIATE

A Roadmap to Compliance

A multi-quarter plan that ties each action to the obligation it satisfies, so progress can be reported as regulatory coverage rather than a list of IT tasks.

You receive: a quarter-by-quarter roadmap, a control-to-regulation mapping, and a board milestone schedule.

Maps to · DORA · GDPR · NIS2 · ISO 27001

05

GOVERN

Board Advisory & Reporting

Standing support between assessments: a defined reporting cadence, a written risk appetite, and an independent voice when the board needs to challenge what it is told.

You receive: a plain-language board report each cycle, a risk appetite statement, and a reviewed risk register.

Maps to · DORA management body duties · GDPR Art. 24

06

GOVERN

Board Training & Cyber Awareness

Director-level literacy sessions that build the confidence to ask the right questions, alongside an organisation-wide awareness programme for the people threats reach first.

You receive: board briefing sessions, a question set for challenging providers, an awareness programme and attendance evidence for your file.

Maps to · DORA ICT training for the management body · GDPR Art. 39

WHERE DOES YOUR BOARD STAND TODAY?

Three questions every board should be able to answer

01 Has our security posture been independently verified in the last 12 months?

02 Do we have evidence that the institutions and custodians holding our assets or data meet the standards they claim?

03 Can we demonstrate to regulators that we actively govern our cyber and data protection risk?

If the answer to any of these is uncertain, that is precisely where we start.

TALK TO US

Request a confidential briefing

FutureRange helps boards move from anxiety to assurance, turning cyber and data protection risk into a well-governed, strategic advantage.

Daniel Garry
dgarry@futurerange.ie
www.futurerange.ie

FUTURE RANGE
PART OF MENTORA GROUP

Protect · Empower · Evolve